CLAIMS

1. A wireless ad-hoc communication system constituted by a plurality of terminals, comprising:

a first terminal that encrypts a payload of a broadcast frame and that transmits the broadcast frame; and

a second terminal that receives the broadcast frame and that decodes the payload of the broadcast frame,

wherein the first terminal encrypts the payload of the broadcast frame using a broadcast encryption key of the first terminal, and

the second terminal decodes the payload of the broadcast frame using the broadcast encryption key of the first terminal.

2. The wireless ad-hoc communication system according to claim 1, wherein the second terminal includes:

an encryption-key management list table having at least an encryption-key management list comprising a set of a terminal identifier of the first terminal and the broadcast encryption key of the first terminal;

means for searching the encryption-key management list table based on the terminal identifier of the first terminal included in a start-terminal identifier of the received broadcast frame to extract the corresponding broadcast

encryption key of the first terminal; and

means for decoding the payload of the broadcast frame using the extracted broadcast encryption key of the first terminal.

3. The wireless ad-hoc communication system according to claim 1, wherein the first terminal includes:

a generated-key table that stores the broadcast encryption key of the first terminal;

means for encrypting the payload of the broadcast frame using the broadcast encryption key of the first terminal stored in the generated-key table; and

means for transmitting the encrypted broadcast frame.

4. A terminal comprising:

an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key of the different terminal;

means for searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and

means for decoding a payload of the broadcast frame using the extracted broadcast encryption key.

5. A terminal comprising:

an encryption-key management list table having at least one encryption-key management list that stores a unicast encryption key between said terminal and a different terminal and a broadcast encryption key of the different terminal in association with a terminal identifier of the different terminal;

means for, when an end-terminal identifier of a received frame is a broadcast address, searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of the frame to extract the corresponding broadcast encryption key as an encryption key, and when the end-terminal identifier of the received frame is other than a broadcast address, searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of the frame to extract the corresponding unicast encryption key as the encryption key; and

means for decoding a payload of the frame using the extracted encryption key.

6. A terminal comprising:

a generated-key table that stores a broadcast encryption key of said terminal;

means for encrypting a payload of a broadcast frame using the broadcast encryption key; and

means for transmitting the encrypted broadcast frame.

7. A terminal comprising:

a generated-key table that stores a broadcast encryption key of said terminal;

an encryption-key management list table having at least one encryption-key management list that stores a unicast encryption key between said terminal and a different terminal in association with a terminal identifier of the different terminal;

means for, when a frame to be transmitted is a broadcast frame, encrypting a payload of the broadcast frame using the broadcast encryption key of the generated-key table, and when the frame to be transmitted is a unicast frame, searching the encryption-key management list table for the encryption-key management list including an end-terminal identifier of the unicast frame to encrypt a payload of the unicast frame using the corresponding unicast encryption key; and

means for transmitting the encrypted frame.

8. A terminal comprising:

means for encrypting a terminal identifier and a

broadcast encryption key of said terminal using a unicast encryption key of a transmission-destination terminal; and

means for transmitting the encrypted terminal identifier and broadcast encryption key of said terminal to the transmission-destination terminal.

9. A terminal comprising:

an encryption-key management list table having at least one encryption-key management list that stores a broadcast encryption key of a different terminal in association with a terminal identifier of the different terminal;

means for encrypting the encryption-key management list using a unicast encryption key of a transmission-destination terminal; and

means for transmitting the encrypted encryption-key management list to the transmission-destination terminal.

10. A terminal comprising:

means for receiving a terminal identifier and a broadcast encryption key of a different terminal from the different terminal;

means for encrypting the terminal identifier and the broadcast encryption key of the different terminal using a broadcast encryption key of said terminal; and

means for broadcasting the encrypted terminal

identifier and broadcast encryption key of the different terminal.

11. A method for decoding a broadcast frame in a terminal that includes an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key of the different terminal, the method comprising the steps of:

searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and

decoding a payload of the broadcast frame using the extracted broadcast encryption key.

12. A method for encrypting a broadcast frame in a terminal that includes a generated-key table storing a broadcast encryption key of said terminal, the method comprising the steps of:

encrypting a payload of the broadcast frame using the broadcast encryption key stored in the generated-key table; and

transmitting the encrypted broadcast frame.

13. A method for distributing a broadcast encryption key in a second terminal, comprising the steps of:

receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key;

encrypting a terminal identifier and a broadcast encryption key of the second terminal using the unicast encryption key; and

transmitting the encrypted terminal identifier and broadcast encryption key of the second terminal to the first terminal.

14. A method for distributing a broadcast encryption key in a second terminal, comprising the steps of:

receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key;

encrypting the terminal identifier and the broadcast encryption key of the first terminal using a broadcast encryption key of the second terminal; and

transmitting the encrypted terminal identifier and broadcast encryption key of the first terminal to a third terminal.

15. A program that causes a terminal including an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key of the different terminal to execute the steps of:

searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and

decoding a payload of the broadcast frame using the extracted broadcast encryption key.

16. A program that causes a terminal including a generated-key table that stores a broadcast encryption key of said terminal to execute the steps of:

encrypting a payload of a broadcast frame using the broadcast encryption key stored in the generated-key table;

and

transmitting the encrypted broadcast frame.

17. A program that causes a second terminal to execute the steps of:

receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key;

encrypting a terminal identifier and a broadcast encryption key of the second terminal using the unicast encryption key; and

transmitting the encrypted terminal identifier and broadcast encryption key of the second terminal to the first terminal.

18. A program that causes a second terminal to execute the steps of:

receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key;

encrypting the terminal identifier and the broadcast encryption key of the first terminal using a broadcast encryption key of the second terminal; and

transmitting the encrypted terminal identifier and broadcast encryption key of the first terminal to a third terminal.